

REMARKS

In the Official Action mailed 23 August 2007, the Examiner reviewed claims 1-4, 6-11, 13-18 and 20-30. The Examiner has rejected claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph; and has rejected claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a).

Applicant submits that the present amendment should be entered because it addresses issues that had not been raised before the final rejection. Accordingly, this is the first opportunity for applicant to address these issues, and this amendment should be entered because essentially it complies with a requirement of form set forth for the first time in the Final Office Action. 37 C.F.R. §1.116(b)(1).

Applicant has amended claims 23, 24, 26, 27, 29 and 30. Claims 1-4, 6-11, 13-18 and 20-30 remain pending.

The rejections are respectfully traversed below and reconsideration is requested.

Rejection of Claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential elements. Without acquiescing in the basis for this rejection, Applicant has added steps to each of these claims by which the "first station" performs the omitted element.

Accordingly, reconsideration of the rejection of claims 23, 24, 26, 27, 29 and 30 as amended is respectfully requested.

Rejection of Claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a)

The Examiner has rejected claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a) as being unpatentable over Perlman (US 6,363,480), and further in view of Kelly (US 5,636,280).

Applicant submits that the assertions in the Office Action are mistaken about the scope and content of the cited prior art, and about the differences between the claims and the prior art. Accordingly, the Examiner's rationale for concluding that the claims are obvious is flawed, and reconsideration is requested.

Basic misunderstandings of the prior art or the claims include:

(1) Contrary to positions stated in the Office Action, Perlman and the SSL protocol mentioned in Perlman do not relate to distribution of session-specific symmetric keys, do not relate to mutual authentication, and do not teach the use of a session key (a name given in the present application to a first key used in the set of exchanges) followed by a set of intermediate keys all produced at the first station, in a process of delivering a symmetric key, also produced at the first station, to the second station.

(2) Contrary to positions stated in the Office Action, Kelly does not describe system of a plurality of exchanges for verification of a key as required in the claims. Rather Kelly describes a system using a plurality of exchanges to verify a password. The claims herein recite a process that never requires sending secret credentials, like passwords, over communication lines, either in clear text or encrypted. Therefore, verification of secret credentials, like Kelly teaches, is not part of the claims herein.

Turning to specific parts of the Office Action, starting with the first part of paragraph 7.1, Perlman is characterized as disclosing "a method for producing ephemeral, symmetric encryption keys at a first station for mutual authentication and secure distribution of random session specific symmetric encryption key in a communication session with a second station..." (page 3). There are two parts to this allegation that the preamble of claim 1 is disclosed in Perlman, both of which are incorrect.

Perlman does not address "mutual authentication" in any sense. The word "mutual" is not present anywhere in Perlman's specification or claims, neither literally nor in essence. Moreover, just the word "authentication" (or "authenticated") alone is not met in the specification and in the claims, except col.1, line 34 where, in the Background of the Invention section, Perlman makes the statement that "... authentication permits the recipient to verify the source of the message", and col. 2, line 22 of the same section, where the known SSL protocol is mentioned as providing "... authenticated, private, real-time communication." This absence of discussion of authentication is not surprising given the fact that Perlman invention does not need either mutual authentication or user authentication for the main embodiments presented in Figs. 1, 3, and 6 based on public and private key pairs. A public key, chosen by the second station due to the timing requirements and used to encrypt a message at the second station, is not a secret. Hence, there is no issue of authentication involved in the transfer of a public key from the first

station to the second station. Since the private key used to decrypt the message is with the first station to begin with, there is no need for any kind of authentication in the process of Perlman.

The second mistake in the characterization that Perlman discloses the subject matter of the preamble, is that Perlman does not describe a process for "secure distribution of random session specific symmetric encryption keys." The closest that Perlman comes to this technology is to state that if a symmetric encryption key is utilized as an alternative to the public key infrastructure of Perlman's preferred embodiment, "When an ephemeral symmetric key is provided to the second party, it should be conveyed in a secure manner, for example through a conventional encrypted tunnel mechanism." (Perlman column 6, lines 17-20). There is no description of a process for distributing symmetric keys in Perlman.

The main embodiments of Perlman are based on asymmetric key pairs, which, as stated above, do not require a secure distribution of the private key because it always remains at the first station. Second, in a case of a symmetric key, its secure distribution cannot be achieved without mutual authentication of the first station and a second station, and such mutual authentication is not described in Perlman.

Perlman just postulates existence at the first station of a variety of ephemeral keys with different expiration times, which a user or a device at a second station can choose from – it is totally unrelated to a secure symmetric key distribution between the first station and a second station.

The present invention provides something entirely different than Perlman. The subject matter recited in the preamble of claim 1, including a secure symmetric encryption key distribution between stations and mutual authentication is a subject matter not touched in Perlman. The comment in the Office Action to the contrary is clearly mistaken.

In paragraph 7.1, first bullet, of the Office Action, the step of "assigning a session key in the first station..." is alleged to be met by "the SSL protocol as exemplified in Perlman col. 2 lines 20-35, establishes a session key between the parties of communication." Office Action, page 4. That this is a reference to Perlman col. 2 lines 20-35 in the Background of the Invention section where Perlman discusses the use in the SSL protocol of a well known server-generated, short-time public/private key pairs, which is as an example of a so called "forward security" approach which was developed in the pioneering work by C. Günter, "An identity-based key-exchange protocol", published in G. Brassard, editor. Advances in Cryptography - CRYPTO'89, volume

435 of Lecture Notes in Computer Science, Springer-Verlag, 1990, 20-24 Aug 1989). The Examiner mistakenly uses this reference in Perlman as an example of "... a plurality of exchanges executed for distributing the symmetric encryption key produced for use in the communication session." However, forward security technology has nothing to do with exchanging symmetric keys. To the contrary, it is focused on generating and exchanging public/private key pairs as it was first proposed by A. Back (Non-interactive forward secrecy, 1996. Posting to cypherpunks mailing list (6/9/1996), archived at <<http://cypherpunks.venona.com/date/1996//09/msg00561.html>>. In this SSL protocol described in Perlman, the public key is provided by the first station to the second, and a symmetric key is provided by the second station to the first. This breaks the cycle set forth in the present claims.

In paragraph 7.1, second bullet of the Office Action, the step of "associating, in the first station, a set of intermediate data keys, different from said session key, with said request for use in said plurality of changes" is interpreted as being met by Perlman column 5, lines 55-67. This cited passage is found in the detailed Description of the Invention section where Perlman introduced the algorithm, which is also graphically depicted in Fig. 3, as to how public/private key pairs having different obliteration time in the pair list are employed. This position by the Examiner is clearly erroneous, because the algorithm of Fig. 3 in Perlman is not connected in any way to an SSL protocol on which the Office Action relies for providing a "session key." The SSL protocol relied upon in the Office Action is used for distribution of a public key. A symmetric key used in that protocol, previously distributed in an unknown process and already in the possession of the second station, is delivered to the first station encrypted using the public key. (Perlman, column 2, line 19-24). Accordingly, the claim requirements that the session key be used in "a plurality of exchanges executed for distributing the symmetric encryption key" and that the set of intermediate data keys be associated with the request in the first station "for use in said plurality of exchanges" are not met.

Furthermore, there are a number of additional errors in the interpretation of the "associating..." step relied upon. Here are some of them:

- a. In Perlman, each key pair in the list can be characterized as a session pair. Once the time-limited private key from the pair is obliterated, the messages stored, encrypted with the corresponding public key, cannot ever be decrypted. The time the private key is obliterated is effectively the end of the session. The other pairs in the list are not intermediate ephemeral key

pairs, either in the Perlman sense, or in the sense of our application. As can be seen in Fig. 3, all the steps 40, 42, 44, 46, 48, and 50 are associated only with one key pair selected as a session key pair of the main embodiment of the Perlman algorithm. There is no need for any sort of intermediate data keys in the Perlman algorithm.

b. With respect to the requirement for the use of ephemeral keys as stated in claim 4, for example, a session key in Perlman is an encryption key having a life time that is exactly the same as the session duration. Hence, any key chosen by the second station is not truly ephemeral with respect to the session time. Furthermore, the Perlman key is not ephemeral at the first station as well, because despite each pair having a different time limit (a time obliteration tag) - this time limitation turns on only under condition that the key has been chosen by the second station as a session key. Otherwise, it can stay at the first station with no time limit. Unlike Perlman, in our application, a session key is truly ephemeral at both the first station and the second station. At the first station, if the key is not becoming a session key for a while, it gets obliterated anyway. At the second station, the session key is used for only a fraction of the session time at the beginning of the session.

c. The Examiner apparently believes that once the session key is chosen from the Perlman list of pairs, the other pairs can play the role of intermediate data keys similar to our claims. However, in our claims, the intermediate data keys are used in a plurality of exchanges during a session for distribution of a symmetric key. Clearly, this is not the case in Perlman, where only one key pair is used in a session, distribution of the key is not described, and no key pair in the list is involved in any session using a different key pair.

d. The Examiner is apparently assuming that the algorithm of Fig. 3 is usable for symmetric key distribution. However, this misses a certain disconnect in Perlman between the text in col. 5, lines 55-67 and Fig.3, if one tries to extend the algorithm to symmetric keys. Once Perlman extrapolates the Fig. 3 algorithm to symmetric encryption keys - out of all steps in this algorithm, only the first and last steps can be really implemented. One can imagine revising Fig. 3 so that the first step 40 legend would sound like "First party announces current ephemeral symmetric keys," and the last step 50 legend would sound like "First party destroys ephemeral symmetric key at the expiration time." All other steps in Fig. 3 are not applicable for a secure symmetric key exchange. There is no place in Perlman's specification or figures where an algorithm of exchanging a symmetric key is discussed or introduced, or proposed, except as mentioned above,

where it cites “conventional technology” for distributing symmetric keys, at col. 6, lines 16-20. This issue was critically reviewed in our previous reply, which the Examiner had found persuasive. Thus, Perlman is in reality directed to completely different subject matter than the present claims.

In paragraph 7.1, third bullet, the Office Action appears to concede that Perlman does not describe the limitations in claim 1 describing the “first exchange” and “another exchange in the plurality of exchanges.” Rather, the Office Action relies upon Kelly to provide evidence that such exchanges would have been obvious. As explained above, even if one conceded that Kelly teaches the use of a plurality of exchanges as claimed, there is no key exchange in the Perlman system that could be replaced by such a plurality of exchanges to satisfy the claims.

Furthermore, Kelly does not teach the use of a “... shared parameter being encrypted using said session key to verify receipt of said session key by the second station ...” As explained below, the shared parameter of claim 1 is not a secret that is verified. Rather, encryption of it using the session key establishes that the second station received the session key. Unlike Kelly, the present invention provides a protocol by which secret credentials are never required to be transferred over communication lines, either in clear text or in encrypted form.

The Examiner refers to Kelly col.7, lines 5-50 as follows: “...(authentication of parties of communication to each other and verification of session key based on shared secret was well-known in the art at the time of invention. Kelly col. 7, lines 5-50 provides a matching example. Specifically, after the session key is established, in item (d) of the authentication protocol, a password (shared secret) is encrypted using the session key and sent to the host. The host verifies the password, and authenticates the other party).” The transfer of the encrypted password by Kelly, and the verification of the password by the host, are completely different than the present claims, which require verification of the key. The Examiner’s characterization of Kelly that it shows “verification of session key” is not correct.

Although the claims recite encryption of a shared parameter, in the present invention, it is not the shared parameter that is verified in the plurality of exchanges. Furthermore, as is abundantly clear in the specification of the present application, the shared parameter recited in claim 1 need not be, and is preferably not, a secret client credential.

The Examiner’s point that “... verification of session key based on shared secret was well known in the prior art at the time of invention. ...” is not correct. Kelly employs a dual-key

reflexive encryption scheme (col. 4, lines 44-55) which is based on an encoding/decoding symmetric key permanently stored at the first station and at the second station, and a transitory key generated at the first station and then encrypted with the permanent key and sent to the second station. Then, the second station decrypts the transitory key with the same permanent key and sends the password encrypted with the transitory key to the first station. Eventually, the first station decrypts the password with the session key, compares it with the stored password at the first station and makes yes/no authentication decision. Clearly, the whole this scheme is not a session key verification but a password verification process made somewhat secure with the session key. The Examiner had misrepresented the subject matter of the prior art.

Kelly's patent was issued in 1997. Since that time, it is generally accepted in the industry that storing permanent static symmetric keys at both stations is a very serious cause of insecurity - it is very difficult to protect the keys themselves from being stolen or compromised in the networked environment. Moreover, using the same permanent keys a number of times helps intruder's efforts to re-engineer these keys with offline computer-processing attacks. As a matter of fact, considered altogether, it weakens the security of the session key (transitory key in Kelly) distribution between the stations and in the end jeopardizes the authentication security.

Most likely, the Examiner had misinterpreted our application claim 1 by assuming that "the shared parameter" in claim 1 is a shared secret between stations (like a password), whereas in reality the specification describes use of either a user name of the user at the second station or the second station's host ID - which are not secret credentials. That is one of the reasons why the reference to Kelly is incorrect and cannot be "a matching example." Claim 1 recites "..., the shared parameter being encrypted using said session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station, ..."

Accordingly, the Examiner's reference to item (d) in Kelly (col.7, lines 34-37) which is describing an authentication step of sending a password encrypted with a session key from the second station to the first station to verify the password does not teach the claimed limitation. In fact, the Kelly requirement for transferring a password on the communication lines is not similar to the invention claimed herein, which avoids transferring any authentication credentials either in a clear text or in an encrypted form over communication lines. In other words, secret credentials in the claimed architecture are not required to be in transit ever, in any form.

Finally, the Examiner's rationale set forth on page 5, for finding obviousness relies on clear mistakes about the teaching of the prior art. We address the rationale sentence by sentence.

The Examiner states, "At the time of invention, it would have been obvious to the person skilled in the art to combine the method of secure key exchange as taught by Kelly with the method of ephemeral key distribution as taught by Perlman." This sentence includes two mistakes. First, Kelly teaches secure password or challenge/response exchange rather than secure key exchange as required in the claims. (See Kelly, Fig. 4). Second, Perlman does not describe distribution of symmetric keys as required in the claims.

The second sentence in the rationale for finding obviousness reads: "Kelly teaches the method to securely deliver keys from one party to another." As explained in detail above, this conclusion is simply not correct.

The third sentence in the rationale for finding obviousness reads: "Perlman teaches the use of multiple ephemeral keys to secure the communication session, which requires transmission of ephemeral keys from one party to the other." Again, this is clearly mistaken. Perlman teaches the use of a single pair of keys in the case of public/private key pairs for each session, only one of which is a public key that is distributed to the second party. In Perlman, the case of using a symmetric key is never described, but presumably a single symmetric key would be used in each session. There is no procedure in Perlman involving the use of multiple keys.

The fourth sentence in the rationale for finding obviousness reads: "Therefore, one skilled in the art would be motivated to use the method of Kelly to deliver the ephemeral keys of Perlman from one party to the other." This combination would not yield the present invention.

Accordingly, the evidence in this record does not suggest obviousness of the claims. The rationale for the finding of obviousness that is set forth is based on a misunderstanding of either the references or the claims or both. For this reason, Applicant submits that the rejection should be withdrawn and the application passed to allowance.

The differences between Perlman and the other claims is set forth in detail in the previous arguments presented by Applicant, and not repeated here. The Kelly reference does not overcome these deficiencies.

In connection with dependent claims 23 and 24 (and 26, 27, 29 and 30 which are similar), the Examiner asserts that the rejection of claim 1 essentially addresses all limitations in these

dependent claims. Applicant submits that this conclusion is clearly incorrect, for the reasons set forth above with respect to the Perlman and Kelly references.

The Examiner characterizes claim 23 as simply reciting the use of an iterative method to improve a cryptographic protocol and alleges that the use of such iterative techniques "to improve the security of the cryptographic protocol is well known in the art." First, Applicant points out that the present invention is not a cryptographic protocol for an iterated cryptosystem in which a cryptographically weak transformation is applied repeatedly to a message, so that the composed transformation is strong. For instance, a DES encryption/decryption algorithm consists of 16 rounds of a transformation designed to fully mix message information together with random key information. In our application, it is rather a protocol for secure distribution of a symmetric encryption key and mutual authentication of the first station and the second station. Rejecting claim 23 on the basis that there is an iterative technique known in a cryptography field unrelated to our application seems to be a profound misinterpretation of both - the actual subject matter and the cited prior art.

Second, if the Examiner intended to assert that the use of the iterative techniques for distribution of symmetric keys and mutual authentication of the first and the second station as recited in the claims herein, is well known in the art, then Applicant specifically requests that evidence be provided to support these allegations.

The references in the Office Action to the DES protocol and to the SKEY, to support the assertion of well known prior art, are inapposite. The DES protocol as described in the Office Action is an encryption protocol, having nothing to do with the distribution of the symmetric keys between two remote stations and their concurrent mutual authentication. The SKEY described in the cited passage of the Schneier text is not an iterative algorithm for distributing a key and a mutual authentication of two parties in any sense. In fact, the SKEY algorithm as described in the citation depends on giving the client a list of numbers in advance without any iterative distribution algorithm. Furthermore, the numbers in SKEY are used simply as passwords, rather than as symmetric keys for use in a communication session as claimed herein. Therefore, the reasoning upon which the Examiner bases the allegation that iterative techniques are well known in the art for distribution of symmetric keys (if this is what the examiner intended), is not supported by a clear line of reasoning and should be withdrawn.

Alternatively, Applicant demands under the provisions of MPEP 2144.03 Reliance on Common Knowledge in the Art or "Well Known" Prior Art, that the Examiner provide documentary evidence to support this unfounded conclusion.

Accordingly, reconsideration of the rejection of claims 1-4, 6-11, 13-18 and 20-30 as amended is respectfully requested.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1005-1).

Respectfully submitted,

Dated: 23 October 2007

/Mark A. Haynes/
Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax